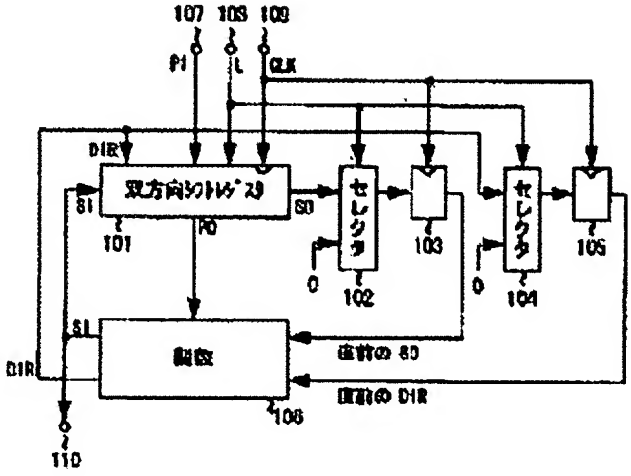
NON-LINEAR FEEDBACK SHIFT REGISTER CIRCUIT

Publication number: JP10320181
Publication date: 1998-12-04
Inventor: SHIMADA MICHIO
Applicant: NIPPON ELECTRIC CO
Classification:
- international: ***G06F7/58; G09C1/00; H03K3/84; H04L9/26;*** **G06F7/58; G09C1/00; H03K3/00; H04L9/18;** (IPC1-7): G06F7/58; G09C1/00; H03K3/84; H04L9/26
- European: G06F7/58P1
Application number: JP19970146072 19970521
Priority number(s): JP19970146072 19970521

Also published as:
EP0887728 (A2)
US6067359 (A1)
EP0887728 (A3)
CA2238294 (C)

Abstract of **JP10320181**

PROBLEM TO BE SOLVED: To attain a non-linear feedback shift register circuit allowed to be reduced at its circuit scale and easily designed. SOLUTION: A bidirectional flip flop(FF) 101 shifts an internal state of m bits right or left in accordance with the value '0' or '1' of an output bit DIR from a function generator 106 and outputs a right end or left end bit as a serial output SO. The function generator 106 inputs a parallel output PO from the register 101, a just preceding serial output SO from the register 101 and a just preceding output bit DIR from the generator and outputs output bits SI, DIR. The output bit SI is outputted from an output terminal as a false random number. The design of the non-linear feedback shift register circuit is equivalent to the search of an Euler's function, the sorts of functions to be selected as main functions are various and the scale of the circuit can be reduced.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－320181

(43)公開日　平成10年(1998)12月４日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	7/58		Ｃ０６Ｆ	7/58	Ａ
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ｂ
		６５０			６５０Ｂ
Ｈ０３Ｋ	3/84		Ｈ０３Ｋ	3/84	Ｚ
Ｈ０４Ｌ	9/26		Ｈ０４Ｌ	9/00	６５９

審査請求　有　請求項の数５　ＦＤ　（全９頁）

(21)出願番号　特願平9－146072

(22)出願日　平成９年(1997)５月21日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝五丁目７番１号　日本電気株式会社内

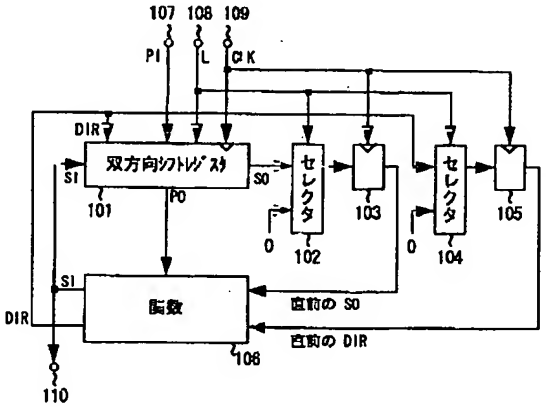
(74)代理人　弁理士　鈴木　康夫

(54)【発明の名称】　非線形フィードバック・シフトレジスタ回路

(57)【要約】

【課題】　回路規模の小型化が可能であり、かつ設計の容易な非線形フィードバック・シフトレジスタ回路を実現する。

【解決手段】　双方向フリップフロップ１０１は、関数発生器１０６の出力ビットＤＩＲの値が０又は１に応じてｍビットの内部状態を右又は左にシフトするとともに、右端又は左端のビットをシリアル出力ＳＯとして出力する。関数発生器１０６は、双方向シフトレジスタ１０１のパラレル出力ＰＯと双方向シフトレジスタ１０１の直前のシリアル出力ＳＯと関数発生器１０６の直前の出力ビットＤＩＲを入力して、出力ビットＳＩと出力ビットＤＩＲを出力する。出力ビットＳＩは疑似乱数として出力端子１１０から出力される。本発明の非線形フィードバック・シフトレジスタ回路の設計は、オイラー閉路を探索することと等価であり、主関数として選べる関数の種類が多様となり、かつ回路規模の小型化が可能である。



【特許請求の範囲】
【請求項１】　少なくとも、後述の関数発生器の第２の出力ビットの値が０あるいは１であるかに応じて、クロック信号が入力される毎に、保持されたｍビットのビット系列を右あるいは左にシフトするとともに、ビット系列を右にシフトする際には、ビット系列の右端のビットをシリアル出力信号として出力して、前記関数発生器の第１の出力ビットをビット系列の左端に保持し、ビット系列を左にシフトする際には、ビット系列の左端のビットをシリアル出力として、前記関数発生器の第１の出力ビットをビット系列の右端に保持し、かつ、保持されているｍビットのビット系列をパラレル出力信号として出力する双方向シフトレジスタと、
前記クロック信号が入力される毎に前記双方向シフトレジスタの前記シリアル出力信号を保持して保持された値を出力する第１のフリップフロップと、
前記クロック信号が入力される毎に前記関数発生器の第２の出力ビットを保持して保持された値を出力する第２のフリップフロップと、
前記双方向シフトレジスタのパラレル出力信号と前記第１のフリップフロップの出力信号と前記第２のフリップフロップの出力信号に依存して第１の出力ビットと第２の出力ビットを出力する前記関数発生器と、から構成され、前記クロック信号が入力される毎に前記関数発生器の第１の出力ビットを疑似乱数として出力することを特徴とする非線形フィードバック・シフトレジスタ回路。
【請求項２】　前記関数発生器は、前記双方向シフトレジスタのパラレル出力信号に依存してそれぞれ１ビットを出力する第１の関数発生器および第２の関数発生器と、前記第１の関数発生器の出力と前記第１のフリップフロップの出力との排他的論理和を計算して計算結果を前記第１の出力ビットとして出力する第１の排他的論理和回路と、前記第２の関数発生器の出力と前記第２のフリップフロップの出力との排他的論理和を計算して計算結果を前記第２の出力ビットとして出力する第２の排他的論理和回路とから構成されていることを特徴とする請求項１記載の非線形フィードバック・シフトレジスタ。
【請求項３】　前記第１の関数発生器は、前記双方向シフトレジスタのパラレル出力信号に依存してそれぞれ１ビットを出力する主関数発生器及び補助関数発生器と、この主関数発生器の出力と補助関数発生器の出力の排他的論理和を計算して計算結果を出力する排他的論理和回路とから構成されていることを特徴とする請求項２記載の非線形フィードバック・シフトレジスタ回路。
【請求項４】　前記主関数発生器は論理回路によって構成され、前記補助関数発生器は論理回路又はリード・オンリ・メモリ（ＲＯＭ）によって構成されていることを特徴とする請求項３記載の非線形フィードバック・シフトレジスタ回路。
【請求項５】　前記各関数発生器の入力である前記双方向シフトレジスタのパラレル出力データとそれに対応する前記各関数発生器の出力データを記録した請求項１、２、３又は４記載の非線形フィードバック・シフトレジスタに用いる記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信装置や情報処理装置において採用され、許可されていないものが通信データや記録媒体の内容を読みとることを困難にするために、送信データ系列に疑似乱数を排他的論理和で足し込む、ストリーム暗号を作成するための非線形フィードバック・シフトレジスタ回路に関するものである。
【０００２】
【従来の技術】ストリーム暗号とは、送信データ系列に疑似乱数を排他的論理和で足し込むことによって、疑似乱数の値を知らない第三者によって送信データが読みとられることを防止するものである。
【０００３】このストリーム暗号における疑似乱数を生成する方法として、非線形フィードバック・シフトレジスタ回路を用いる方法が古くから使われている。図９は、従来の非線形フィードバック・シフトレジスタ回路の基本構成を示す機能ブロック図である。
【０００４】図９において、シフトレジスタ９０１は、入力端子９０８から供給される制御信号Ｌが０の時に入力端子９０９からクロック信号ＣＬＫが供給されると、入力端子９０７から供給されるｍビットのビット列ＰＩを内部状態として保持し、入力端子９０８から供給される制御信号Ｌが１の時に入力端子９０９からクロック信号ＣＬＫが供給されると、保持されている内部状態を右に１ビットシフトするとともに内部状態の左端には関数発生器９０２から供給されるシリアル入力ＳＩが保持される。
【０００５】シフトレジスタ９０１の内部状態は、パラレル出力ＰＯとして関数発生器９０２に供給される。また、関数発生器９０２の出力は、疑似乱数として出力端子９１０から出力される。関数発生器９０２は、リード・オンリ・メモリ（ＲＯＭ）あるいは論理回路によって構成される。
【０００６】図１０は、シフトレジスタ９０１の基本構成を示す機能ブロック図である。図１０において、セレクタ1001_1～1001_mは、入力端子１００５を介して供給される制御信号Ｌの値に応じてその左側から供給される２つの入力（上から順にＡ入力、Ｂ入力とする）の一方を選択して右側へ出力する。即ち、セレクタ1001_1～1001_mは、制御信号Ｌが０であればＡ入力を選択して出力し、制御信号Ｌが１であればＢ入力を選択して出力する。
【０００７】入力端子１００７にはｍビットのパラレル入力ＰＩが供給され、ＰＩのそれぞれのビットがセレクタ1001_1～1001_mのＡ入力に供給される。また、

入力端子１００８から供給されるシリアル入力ＳＩが、セレクタ1001_1のＢ入力に供給される。フリップフロップ1002_1～1002_{m-1}の出力は、セレクタ1001_2～1001_mのＢ入力に供給される。フリップフロップ1002_1～1002_mは、入力端子１００６からクロック信号ＣＬＫが供給される毎に、それぞれ図の左側のセレクタ1001_1～1001_mの出力を保持して、保持した値を図の右側へ出力する。フリップフロップ1002_1～1002_mの出力は、ｍビットのパラレル出力ＰＯとして出力端子１０１０から出力される。したがって、シフトレジスタの内部状態はフリップフロップ1002_1～1002_mに保持されたビット系列によって表される。

【０００８】シフトレジスタの内部状態を設定するには、まず内部状態として設定するｍビットのデータをパラレル入力ＰＩとして入力端子１００７に供給し、入力端子１００５に供給される制御信号Ｌを０とし、入力端子１００６からクロック信号ＣＬＫを１個供給する。すると、パラレル入力ＰＩの各ビットが対応するフリップフロップ1002_1～1002_mに保持される。

【０００９】シフトレジスタに保持されたｍビットを図の右方向に１ビットだけシフトするには、入力端子１００５に供給される制御信号Ｌを１とする。そして、入力端子１００６からクロック信号ＣＬＫを１個供給する。すると、シフトレジスタに保持されたｍビットが図の右方向に１ビットだけシフトする。なお、その際には、入力端子１００８から供給されたシリアル入力ＳＩが左端のフリップフロップ1002_1に保持される。

【００１０】図１０のシフトレジスタの内部状態の可能な変化の仕方は、図１１のような状態グラフによって表現することができる。図１１は、ｍ＝３の場合のシフトレジスタの状態グラフである。図１１において、丸印の中に書かれている３文字は、図９又は図１０のシフトレジスタの内部状態を表している。丸印と丸印の間の矢印の付いた実線は状態の変化の方向を表しており、各実線に添えられている数字０又は１は、シフトレジスタの左端に供給されるシリアル入力ＳＩの値を示している。また、矢印の付いた点線は状態が変化しないことを示している。

【００１１】例えば、０００が記入された丸印の右側に１があり、その数字の添えられている矢印の付いた実線の端に１００が記入された丸印があるが、これはシフトレジスタのシリアル入力としてＳＩ＝１を供給してシフトレジスタを右にシフトさせると、シフトレジスタの内部状態が０００から１００に変化することを意味している。

【００１２】これをグラフ理論における用語と対比させると、図の丸印がノードに対応し、実線が枝に対応している。したがって、従来の非線形フィードバック・シフトレジスタ回路を設計することは、図１１の状態グラフにおいてハミルトン閉路を求めることに他ならない。ハミルトン閉路とは、全てのノードを１度だけ通過して元のノードに戻るような経路のことである。

【００１３】関数発生器９０２の入力は、シフトレジスタ９０１の内部状態すなわち図１１の丸印の内部の値であり、関数発生器９０２の出力はシフトレジスタ９０１に供給するシリアル入力ＳＩすなわち図１１の矢印の付いた実線に添えられた数字であるから、ハミルトン閉路が決まれば関数発生器９０２の入出力関係も決まる。

【００１４】図１２は、図１１の状態グラフに存在するハミルトン閉路の一例である。図１２において、小さな丸印で囲まれた数字の示す順序で、内部状態０００から実線を矢印の方向にたどって行くと、全ての内部状態を１度だけ通過して、再び内部状態０００に戻ることが分かる。

【００１５】図１３は、図１２のハミルトン閉路に対応する関数発生器９０２の入出力対応を示した表である。図１２の閉路の場合、関数発生器９０２から出力される疑似乱数の１周期の出力は、１１１０１０００となる。

【００１６】なお、従来の非線形フィードバック・シフトレジスタ回路については、例えば、１９８６年にスプリンガー・ヴァーラグから刊行されたルェペル著「アナリシス・アンド・デザイン・オブ・ストリーム・サイファー」(R.A.Rueppel,Analysis and Design of Stream Ciphers, Springer-Verlag,1986)などに詳しい解説がある。また、グラフ理論やハミルトン閉路については、例えば、高橋、藤重著「離散数学」（岩波書店１９８１年）などに詳しい解説がある。

【００１７】

【発明が解決しようとする課題】しかしながら、従来の非線形フィードバック・シフトレジスタ回路は、その設計が難しいという問題があった。すなわち、前記のように、疑似乱数の周期を最大にするような関数を設計することは、ハミルトン経路を探索することに他ならないが、ハミルトン閉路を探索することは難しい問題であることが知られている（例えば、前記「離散数学」参照）。図１１の例のように、ノードが８個しか存在しない場合には、試行錯誤で簡単に経路を発見することができるが、シフトレジスタの段数が大きくなってノードの数が多くなると、設計することは事実上不可能になる。

【００１８】また、仮にハミルトン閉路を発見できたとしても、そのようなハミルトン閉路に対応する関数は、０と１とを等頻度で出力するから、論理圧縮して回路規模を小さくすることは、関数が線形な関数である場合など一部の例外を除けば一般に困難である。

【００１９】本発明は、以上の問題点に鑑み、設計が容易で、かつ回路規模を小さくすることができる非線形フィードバック・シフトレジスタ回路を提供することを目的とするものである。

【００２０】

【課題を解決するための手段】本発明は、双方向にシフトできるシフトレジスタ（以下、双方向シフトレジスタという）を用いて非線形フィードバック・シフトレジスタ回路を構成したことを特徴とするものである。

【００２１】グラフの全ての枝をそれぞれ１度だけ通るような経路は、オイラー経路と呼ばれ、探索することが容易であることが知られている。より厳密に言うと、もし、グラフのノードから出ている枝の数が、どのノードについても２あるいは４であれば、グラフの全ての枝をそれぞれ１度だけ通るような経路が存在し、しかも、そのような経路は簡単に求められることが知られている。これらのことについては、グラフ理論関係の参考書（例えば前記の文献等参照）に詳しい解説がある。

【００２２】後述するように、双方向シフトレジスタを利用して非線形フィードバック・シフトレジスタ回路を設計することは、前記オイラー閉路を探索することに帰着され、よって、非線形フィードバック・シフトレジスタ回路の設計が容易となる。

【００２３】

【発明の実施の形態】図１は、本発明の非線形フィードバック・シフトレジスタの第１の実施の形態を示す機能ブロック図であり、図２は、本発明において用いられる双方向シフトレジスタの基本構成を示す機能ブロック図である。

【００２４】説明の便宜上、最初に双方向シフトレジスタについて説明する。図２において、セレクタ２０１$_1$～２０１$_m$は、入力端子２０４から供給される制御信号ＤＩＲ及び入力端子２０５から供給される制御信号Ｌの各値に応じて、図の左側から供給される３つの入力（図の上から順にＡ入力、Ｂ入力、Ｃ入力とする）を選択し、選択された入力を図の右側へ出力する。セレクタ２０３は、入力端子２０４から供給される制御信号ＤＩＲの値に応じて、図の左側から供給される２つの入力（図の上から順にＢ入力、Ｃ入力とする）を選択し、選択された入力をシリアル出力ＳＯとして出力端子２０９から出力する。

【００２５】セレクタ２０１$_1$～２０１$_m$は、制御信号Ｌが０であればＡ入力を選択して出力し、制御信号Ｌが１で制御信号ＤＩＲが０であればＣ入力を選択して出力し、制御信号Ｌが１で制御信号ＤＩＲが１であればＢ入力を選択して出力する。セレクタ２０３は、制御信号ＤＩＲが０であればＣ入力を選択して出力し、制御信号ＤＩＲが１であればＢ入力を選択して出力する。

【００２６】入力端子２０７にはｍビットのパラレル入力ＰＩが供給され、ＰＩのそれぞれのビットがセレクタ２０１$_1$～２０１$_m$のＡ入力に供給される。また、入力端子２０８から供給されるシリアル入力ＳＩが、セレクタ２０１$_1$のＢ入力とセレクタ２０１$_m$のＣ入力に供給される。

【００２７】フリップフロップ２０２$_1$～２０１$_m$は、入力端子２０６からクロック信号ＣＬＫが供給される毎に、それぞれ図の左側のセレクタ２０１$_1$～２０１$_m$の出力を保持して、保持した値を図の右側へ出力する。フリップフロップ２０２$_1$～２０１$_m$から出力される合計ｍビットの出力は、パラレル出力ＰＯとして、出力端子２１０から出力される。

【００２８】ｍ－１個のフリップフロップ２０２$_1$～２０２$_{m-1}$の出力は、それぞれ図の右側のセレクタ２０１$_2$～２０１$_m$のＢ入力にも供給されている。フリップフロップ２０２$_m$の出力は、セレクタ２０３のＢ入力にも供給されている。ｍ－１個のフリップフロップ２０２$_2$～２０２$_m$の出力は、それぞれ図の左側のセレクタ２０１$_1$～２０１$_{m-1}$のＣ入力にも供給されている。フリップフロップ２０２$_1$の出力は、セレクタ２０３のＣ入力にも供給されている。双方向シフトレジスタの内部状態は、フリップフロップ２０２$_1$～２０２$_m$に保持されたビット系列によって表される。

【００２９】双方向シフトレジスタの内部状態を設定するには、内部状態として設定するｍビットのデータをパラレル入力ＰＩとして入力端子２０７に供給するとともに入力端子２０５に供給される制御信号Ｌを０とし、入力端子２０６からクロック信号ＣＬＫを１個供給する。すると、パラレル入力ＰＩのビットが、それぞれフリップフロップ２０２$_1$～２０２$_m$に保持される。

【００３０】双方向シフトレジスタに保持されたｍビットを図の右方向に１ビットだけシフトするには、まず、入力端子２０５に供給される制御信号Ｌを１とし、入力端子２０４に供給される制御信号ＤＩＲを１とする。その際には、セレクタ２０３はＢ入力を選択するので右端のフリップフロップ２０２$_m$に保持されていたビットがシリアル出力ＳＯとして出力端子２０９から出力される。そして、入力端子２０６からクロック信号ＣＬＫを１個供給すると、双方向シフトレジスタに保持されたｍビットが図の右方向に１ビットだけシフトするとともに入力端子２０８から供給されたシリアル入力ＳＩが左端のフリップフロップ２０２$_1$に保持される。

【００３１】双方向シフトレジスタに保持されたｍビットを図の左方向に１ビットだけシフトするには、まず、入力端子２０５に供給される制御信号Ｌを１とし、入力端子２０４に供給される制御信号ＤＩＲを０とする。その際には、セレクタ２０３はＣ入力を選択するので左端のフリップフロップ２０２$_1$に保持されていたビットがシリアル出力ＳＯとして出力端子２０９から出力される。そして、入力端子２０６からクロック信号ＣＬＫを１個供給すると、双方向シフトレジスタに保持されたｍビットが図の左方向に１ビットだけシフトするとともに入力端子２０８から供給されたシリアル入力ＳＩが右端のフリップフロップ２０２$_m$に保持される。

【００３２】図５は、図２の双方向シフトレジスタの状態グラフをｍ＝３の場合について表したものである。図

5において、丸印の中に書かれている3ビットは、図2の双方向シフトレジスタのフリップフロップに保持されているビットを表している。そして、丸印と丸印が、両端に矢印の付いた実線で結ばれている。また、どの実線の両端にも、1R，1L，0R，0Lの4通りの記号の何れかが添えられている。

【0033】この状態グラフの見方は、例えば、000が記入された丸印の右側に、1Rと言う記号があり、その記号が添えられている実線のもう一方の端に100が記入された丸印があるが、1Rの1はシリアル入力SIの値を示し、1RのRは右シフトを示しており、これは、SI＝1として双方向シフトレジスタを右にシフトさせると、双方向シフトレジスタの内部状態が000から100に変化することを意味している。

【0034】図5の状態グラフは、内部状態000，111に対応するノードからは2本の枝が出ており（同じノードに戻る枝を無視すれば）、それ以外のノードからは4本の枝が出ているので、オイラー閉路が存在する。図6は、図5の状態グラフに存在するオイラー閉路の1例である。図において、小さな丸印で囲まれた数字の示す順序で、内部状態000から実線を辿って行くと、全ての実線を辿って、再び内部状態000に戻ることが分かる。

【0035】図1において、双方向シフトレジスタ101は、前記のように、入力端子108から供給される制御信号Lが0の時に入力端子109からクロック信号CLKが供給されると、入力端子107から供給されるmビットのパラレル入力PIを内部状態として保持し、入力端子108から供給される制御信号Lが1で関数発生器106が出力する制御信号DIRが1の時には、内部状態の右端のビットをシリアル出力SOとしてセレクタ102に供給し、その時に、入力端子109からクロック信号CLKが供給されると、内部状態を右に1ビットだけシフトして、内部状態の左端にシリアル入力SIを保持し、入力端子108から供給される制御信号が1で関数発生器106の出力する制御信号DIRが0の時には、内部状態の左端のビットをシリアル出力SOとしてセレクタ102に供給し、その時に、入力端子109からクロック信号CLKが供給されると、内部状態を左に1ビットだけシフトして、内部状態の右端にシリアル入力SIを保持する。

【0036】また、双方向シフトレジスタ101の内部状態はパラレル出力POとして関数発生器106に供給される。セレクタ102は、入力端子108から供給される制御信号Lが0の時には0を選択して出力し、制御信号Lが1の時には、双方向シフトレジスタ101から供給されるシリアル出力SOを選択して出力し、その出力をフリップフロップ103に供給する。フリップフロップ103は、入力端子109からクロック信号CLKが供給されると、セレクタ102の出力を保持して、保持したビットを関数発生器106に供給する。

【0037】セレクタ104は、入力端子108から供給される制御信号Lが0の時には0を選択して出力し、制御信号Lが1の時には、関数発生器106が出力する制御信号DIRを選択して出力し、その出力をフリップフロップ105に供給する。フリップフロップ105は、入力端子109からクロック信号CLKが供給されると、セレクタ104の出力を保持して、保持したビットを関数発生器106に供給する。

【0038】関数発生器106は、双方向シフトレジスタ101から出力されるパラレル出力POと、フリップフロップ103及び105の出力に依存して、制御信号SIと制御信号DIRを出力する。また、関数発生器106の出力する制御信号SIは、疑似乱数として、出力端子110から出力される。

【0039】なお、フリップフロップ103の出力は、1時刻前、すなわち、入力端子109からクロック信号CLKが入力される前に、双方向シフトレジスタ101が出力していたシリアルデータSOであり、フリップフロップ105の出力は、1時刻前に、関数発生器105が出力していた制御信号DIRである。双方向シフトレジスタ101は、1時刻に1ビットだけしかシフトされないから、それらのデータだけで、双方向シフトレジスタ101の1時刻前の状態が特定できる。このため、双方向シフトレジスタのパラレル出力POと、1時刻前のSO及びDIRだけに依存して、関数発生器106の出力SIとDIRが決定される。

【0040】次に、本発明の非線形フィードバック・シフトレジスタの動作について説明する。最初に、双方向シフトレジスタ101の内部状態の初期状態として設定するmビットのデータをパラレル入力PIとして入力端子107に供給し、入力端子108に供給される制御信号Lを0とし、入力端子109からクロック信号を1個供給する。次に入力端子108に供給される制御信号Lを1とする。するとそれ以降は、入力端子109からクロック信号CLKが1個供給される毎に、出力端子110から疑似乱数のビットが出力される。

【0041】ただし、双方向シフトレジスタ101の内部状態の初期状態を000あるいは111にすると、関数によっては、それ以降の内部状態がずっと000あるいは111になって、内部状態がオイラー閉路に沿って遷移しなくなる。例えば図6の例では、内部状態の初期状態を000にしてしまうと、それ以降の内部状態はずっと000のままである。このため、図1の実施の形態においては、双方向シフトレジスタ101の内部状態の初期状態をオール0やオール1にすることは避ける必要がある。

【0042】関数発生器106は、リード・オンリ・メモリ（ROM）あるいは論理回路によって構成することができる。例えば、図6のオイラー閉路に対応する状態

遷移を実現するには、関数発生器１０６の入力と出力の関係を図７の表のように設定すればよい。双方向シフトレジスタ１０１の内部状態の初期状態によっては図６の実線に添えられて番号と逆順に進むこともあるが、いずれの場合も、初期状態を０００あるいは１１１にしない限り、オイラー閉路に沿って移動する。

【００４３】図３は、本発明の非線形フィードバック・シフトレジスタの第２の実施の形態を示す機能ブロック図である。この実施の形態においては、関数発生器１０６の構成方法が前記第１の実施の形態と異なっているだけで、他の部分は第１の実施の形態と同様である。すなわち、図３においては、フリップフロップ１０３と１０５の出力が、関数発生器１０６ではなく、それぞれ排他的論理和回路３０３と３０４に供給されている。

【００４４】排他的論理和回路３０３においては、フリップフロップ１０３の出力と関数発生器３０１の出力ｆとの排他的論理和が計算され、その計算結果は制御信号ＳＩおよび疑似乱数出力として出力される。また、排他的論理和回路３０４においては、フリップフロップ１０５の出力と関数発生器３０２の出力ｄとの排他的論理和が計算され、その計算結果は制御信号ＤＩＲとして出力される。双方向シフトレジスタ１０１から出力されるパラレルデータＰＯは、関数発生器３０１と３０２にそれぞれ供給される。

【００４５】関数発生器３０１と３０２は、それぞれリード・オンリ・メモリ（ＲＯＭ）あるいは論理回路によって構成される。そして、例えば図６のオイラー閉路に対応する状態遷移を実現する場合には、各関数発生器の出力ｆとｄを、図８の入出力対応表のように設定すればよい。このようにすれば、図３の双方向シフトレジスタの内部状態は、図６のオイラー閉路に沿って移動する。双方向シフトレジスタ１０１の内部状態の初期状態によっては図６に実線に添えられた番号とは逆順に進むこともあるが、いずれの場合もオイラー閉路に沿って移動する。

【００４６】これは、どのようなオイラー閉路についても、内部状態Ｓに対して２つのビットＳＩ（Ｓ），ＤＩＲ（Ｓ）が存在して、ＳＩ＝「直前のＳＯ」＋ＳＩ（Ｓ），ＤＩＲ＝「直前のＤＩＲ」＋ＤＩＲ（Ｓ）という関係が成り立っていることに依るものである。ここで、＋は排他的論理和を意味する。この関係は図７の入出力対応表においても成り立っているこの第２の実施の形態においては、図８に示すように、その入出力対応表は、図７に示す第１の実施の形態における入出力対応表よりも簡単化することができるので、関数発生器をＲＯＭで構成した場合には、メモリ容量を小さくすることができる。また、論理回路で構成した場合には、関数の入力ビット数が少なくなり、回路規模を小さくすることができるとともに、動作に伴う遅延時間も小さくなる。

【００４７】図４は、第２の実施の形態における関数発生器３０１の一例を示すブロック図である。図４において、入力端子４０４から入力されたパラレルデータＰＯは、主関数発生器４０１と補助関数発生器４０２に入力される。主関数発生器４０１は論理回路によって構成され、その入力に依存して１ビットを出力する。補助関数発生器４０２は、ＲＯＭあるいは論理回路によって構成され、その入力に依存して１ビットを出力する。そして、主関数発生器４０１の出力と補助関数発生器４０２の出力との排他的論理和が排他的論理和回路４０３で計算され、計算結果が出力端子４０５から関数の出力として出力される。

【００４８】図４の関数発生器を構成するにあたっては、まず、オイラー閉路を選択する前に、主関数発生器４０１を構成する論理回路を適当に決めておく。その際に、論理回路として回路規模の小さな論理回路を選択する。そして、補助関数発生器４０２と関数発生器３０２の出力ができるだけ０となるようなオイラー閉路を選択する。出力の大部分が０であるような論理回路であれば、論理圧縮することで回路規模あるいはメモリ容量を小さくすることができる。一般に、ｍ段の双方向シフトレジスタの状態グラフには、３の2^m-2乗通りのオイラー閉路が存在することが知られており、上記のような条件を満たすオイラー閉路は高い確率で発見できる。

【００４９】

【発明の効果】本発明は、双方向シフトレジスタを用い、非線形フィードバック・シフトレジスタの設計を、オイラー閉路によって実現しており、かつオール０とオール１以外の任意のバイナリ系列を初期状態として設定できるので、回路設計が容易である。

【００５０】また、双方向シフトレジスタを用いているにもかかわらず、関数発生器の構成を工夫することにより、回路規模を小さくすることができる。

【００５１】さらに、関数として選べる種類が非常に多いので、ストリーム暗号の解読が困難な疑似乱数を多く生成することができ、主関数を秘密にすることによる暗号強度の増加を図ることができる。

【００５２】

【図面の簡単な説明】

【図１】本発明の第１の実施の形態を示す機能ブロック図である。

【図２】双方向シフトレジスタの基本構成を示す機能ブロック図である。

【図３】本発明の第２の実施の形態を示す機能ブロック図である。

【図４】本発明の第２の実施の形態において用いられる複数の関数発生器のうちの一つを示す機能ブロック図である。

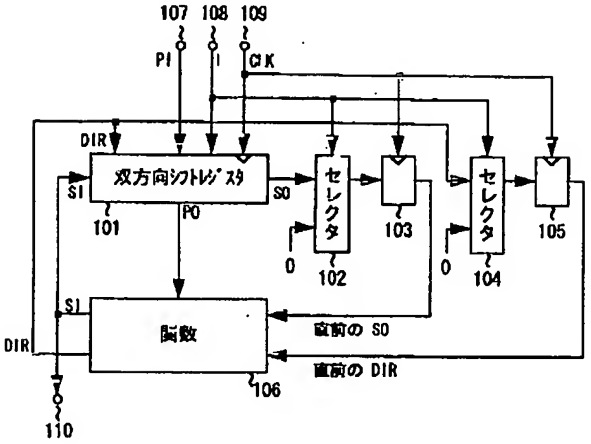
【図５】ｍ＝３の場合の双方向シフトレジスタの状態グラフである。

【図６】図５の状態グラフに存在するオイラー閉路の一

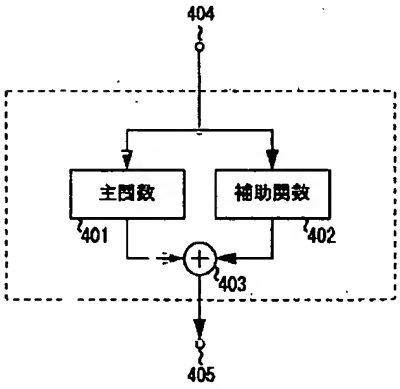
例を示す図である。
【図7】第1の実施の形態における関数発生器に対する図6のオイラー閉路の場合の入出力対応表である。
【図8】第2の実施の形態における関数発生器に対する図6のオイラー閉路の場合の入出力対応表である。
【図9】従来の非線形フィードバック・シフトレジスタ回路を示す機能ブロック図である。
【図10】シフトレジスタに基本構成を示す機能ブロック図である。
【図11】m＝3の場合のシフトレジスタの状態グラフである。
【図12】図11の状態グラフに存在するハミルトン閉路の一例を示す図である。
【図13】従来例における関数発生器に対する図12のハミルトン閉路の場合の入出力対応表である。

【符号の説明】
101　双方向シフトレジスタ
102，104，201，203，1001　セレクタ
103，105，202，1002　フリップフロップ
106　関数発生器
301　第1の関数発生器
302　第2の関数発生器
401　主関数発生器
402　補助関数発生器
303，304，403　排他的論理和回路
901　シフトレジスタ
902　関数発生器

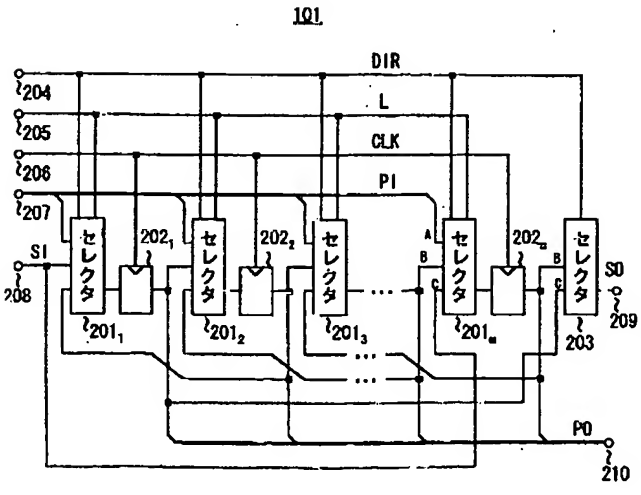
【図1】



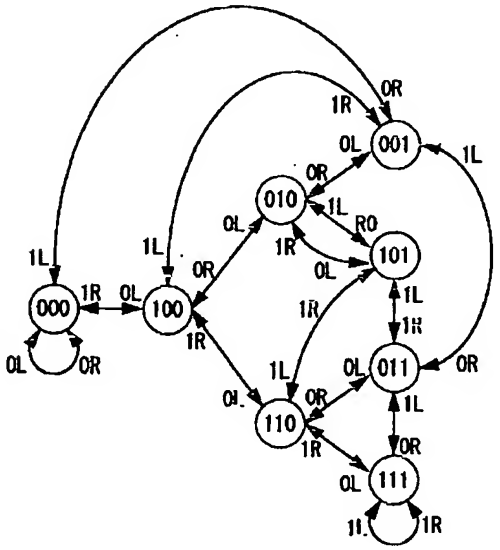
【図4】



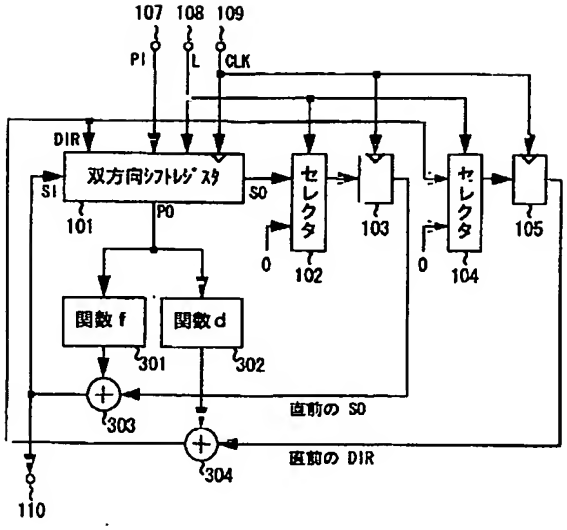
【図2】



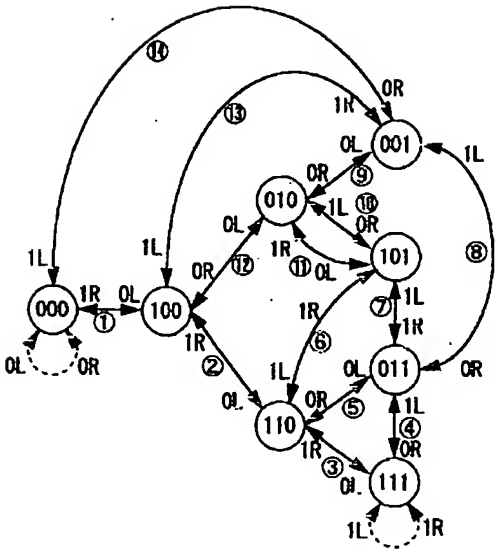
【図5】



【図3】



【図6】



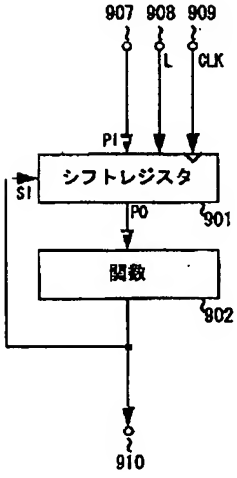
【図7】

PO	直前のSO	直前のDIR	SI	DIR
000	1	1 (R)	1	1 (R)
000	1	0 (L)	1	0 (L)
001	1	1 (R)	0	0 (L)
001	1	0 (L)	0	1 (R)
001	0	1 (R)	1	0 (L)
001	0	0 (L)	1	1 (R)
010	1	0 (L)	0	0 (L)
010	0	0 (L)	1	0 (L)
010	1	1 (R)	0	1 (R)
010	0	1 (R)	1	1 (R)
011	1	1 (R)	0	0 (L)
011	1	0 (L)	0	1 (R)
011	0	1 (R)	1	0 (L)
011	0	0 (L)	1	1 (R)
100	0	1 (R)	1	1 (R)
100	0	0 (L)	1	0 (L)
100	1	0 (L)	0	0 (L)
100	1	1 (R)	0	1 (R)
101	1	0 (L)	1	0 (L)
101	0	0 (L)	0	0 (L)
101	1	1 (R)	1	1 (R)
101	0	1 (R)	0	1 (R)
110	0	1 (R)	1	1 (R)
110	0	0 (L)	1	0 (L)
110	1	0 (L)	0	0 (L)
110	1	1 (R)	0	1 (R)
111	0	1 (R)	0	1 (R)
111	0	0 (L)	0	0 (L)

【図8】

PO	f	d
000	0	0
001	1	1
010	1	0
011	1	1
100	1	0
101	0	0
110	1	0
111	0	0

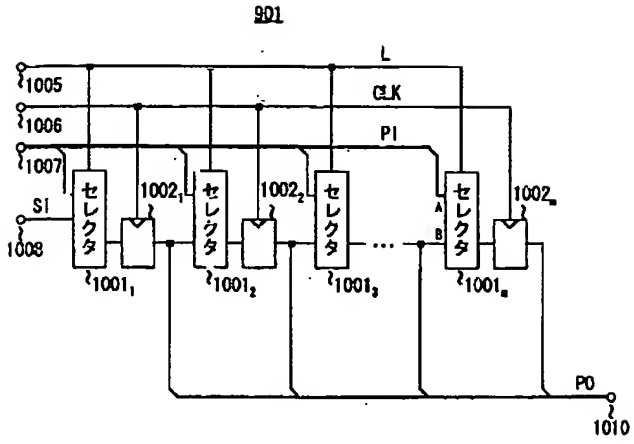
【図9】



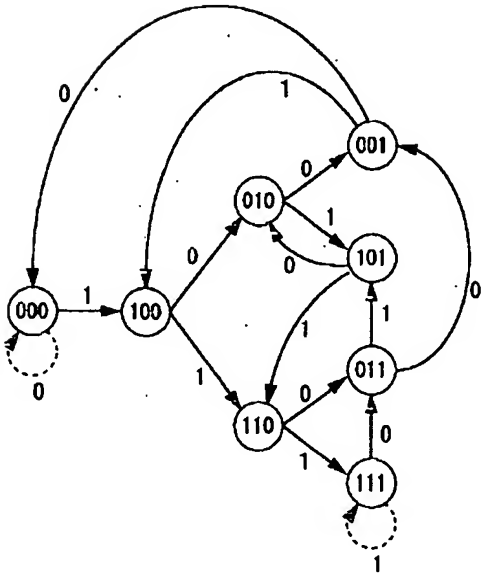
【図13】

PO	関数の出力
000	1
001	0
010	0
011	1
100	1
101	0
110	1
111	0

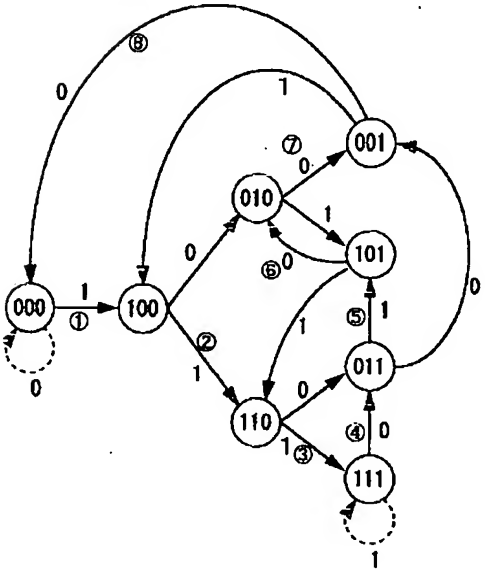
【図10】


901
L
CLK
PI
1005
1006
1007
SI
1008
セレクタ
1002₁
1002₂
1002ₙ
1001₁
1001₂
1001₃
1001ₙ
A
B
PO
1010

【図11】


000
100
001
010
101
011
110
111

【図12】


000
100
001
010
101
011
110
111
①
②
③
④
⑤
⑥
⑦
⑧